IDC MarketScape

IDC MarketScape: Asia/Pacific Managed Security Services 2022 Vendor Assessment

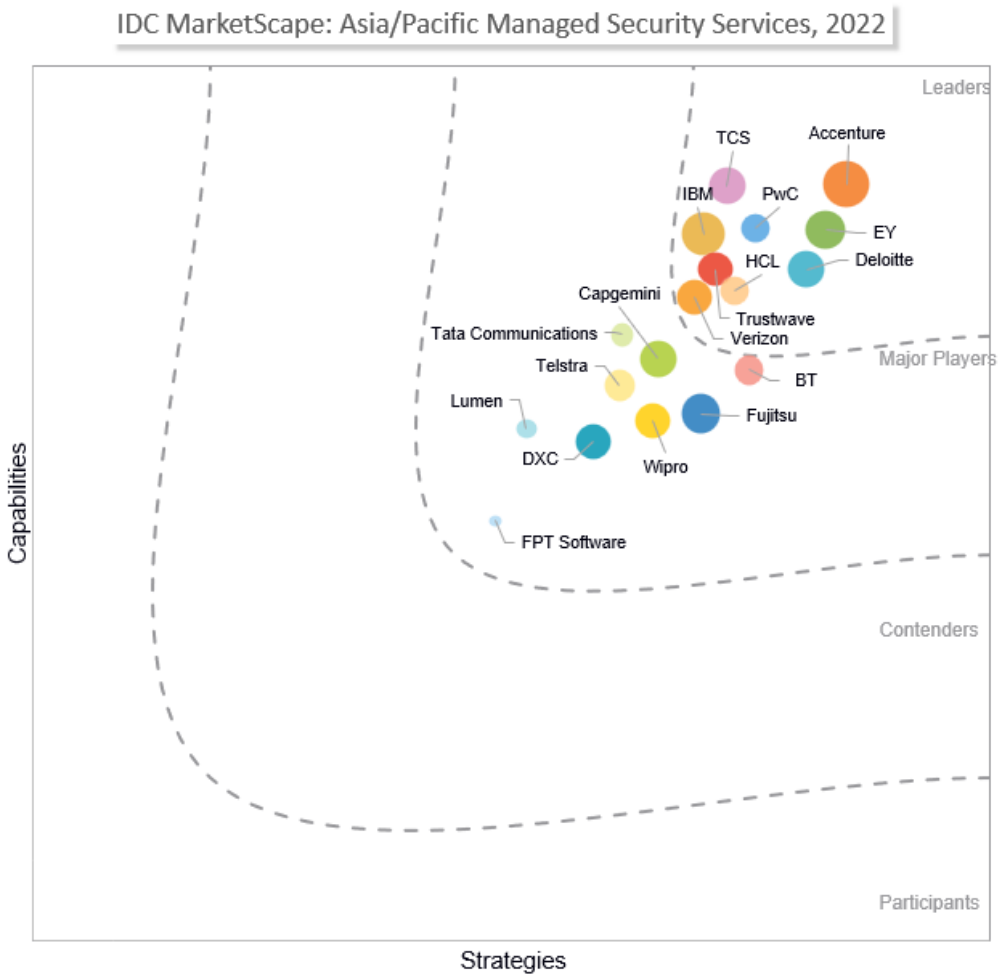
Shweta Baidya Christian Fam

THIS MARKETSCAPE EXCERPT FEATURES: TATA COMMUNICATIONS

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Asia/Pacific Managed Security Services 2022



Source: IDC, 2022

November 2022, IDC #AP49101222e

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly IDC MarketScape: Asia/Pacific Managed Security Services 2022 Vendor Assessment (Doc #AP49101222e). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Advice for Technology Buyers, Featured Vendor Profile, Appendix and Learn More. Also included are Figure 1 and Figure 2.

IDC'S OPINION

The evolving economic and geopolitical uncertainties around the world have forced enterprises to reevaluate their IT strategies and move to a more secure, robust, and digital-first business model. In the race to adapt and evolve to a new environment after the pandemic, enterprises have become increasingly vulnerable to threats and attacks, clearly evident from the rise in ransomware, malware, and phishing attacks, among many others. The complex and hybrid IT environment spanning multiple/hybrid clouds have only added to enterprises' woes. This brought in a higher degree of maturity, and cybersecurity became the center of boardroom discussions with strong funding and leadership support. According to IDC's *2022 Future Enterprise Resiliency and Spending (FERS) Survey* conducted in August 2022, vulnerability assessment, security training, and managed detection and response (MDR) services received the maximum funding to strengthen organizations' cyber-readiness and defense.

With an increase in the number of projects around digital and cloud transformations, enterprises are now working hand in glove with their managed security SPs (MSSPs) to secure their transformation journey and take a more proactive than reactive approach toward threat management. The market is evolving and maturing at breakneck speed, and enterprises expect their partners to provide advisory, consulting, and managed services to identify gaps in their security environment and help them. This has resulted in many SPs adding distinct capabilities around professional security services to cater to their customers' needs.

This IDC study evaluates managed security services vendors in the Asia/Pacific region based on various breadth of offering, threat management capabilities, cloud security expertise, go-to-market activities, and thought leadership. The study assesses their growth in the region across all the key parameters along with strategies for the future. The key findings of the research encompass:

- **A bouquet of services offered under one roof**. Some of the managed security services vendors differentiated themselves by offering extended services, including managed risk, operational technology (OT)/Internet of Things (IoT) managed security, cloud security, supply chain cyber-risk, and security architecture as a service. Enterprises are seeking long-term partners that can support them in their transformational journeys over the next few years. Hence, they are looking beyond the current value proposition showcased by SPs and keenly observing their road map and strategic investments before partnering with them. Further, industry-specific offerings, use cases, and technology innovations are some of the other aspects that

enterprises consider. As a result, MSSPs in the region significantly doubled down on their service offerings and capabilities in line with the rising demand.

- **Thought leadership and innovative thinking**. A strategy that clearly demarcates some of the leading SPs from others is a focus on innovation and thought leadership. With the continuous expansion of the threat landscape, enterprises welcome any initiatives launched by their SPs to share threat intelligence or point of view (POV) on cloud security, ransomware attacks, and OT/IoT attacks. Many vendors have strong industry and government alliances that help them strengthen their threat management capabilities. Vendors that reached out to their customers proactively with risk assessment advisory and actionable insights on how to better secure their assets in future were rated much higher than others. Another interesting trend was the power of co-innovation along with customers and partners. Many vendors are working together with their customers in specific industries to understand their pain points and co-create and codevelop solutions together. The joint ownership model acts as a win–win for both the customer and the MSSP, with the partnership expanding over multiple years.
- **Global capabilities delivered locally or a "glocal" delivery model.** A distinguishing factor among all the participating MSSP was their global capabilities customized for local clients, with the help of regional cybersecurity centers (CSC) and local skill sets. As the region is diverse with respect to culture, language, and social construct, it requires a localization of services to manage client expectations. MSSPs understand this need and are increasingly setting up local innovation and delivery hubs with a healthy balance of global and local teams to leverage global expertise at the regional level. There is a strong focus to build capability centers nearshore to deliver service excellence and gain client confidence and trust.
- **Enhanced portfolio and emerging technologies**. Many of the professional security services (PSS) firms evaluated in this study have extensive offerings beyond basic security services. As the threat landscape becomes increasingly more complex, many PSS firms in the study are heavily investing in emerging technologies, such as secure access service edge (SASE), IT/OT convergence, hybrid cloud platforms, and automation, to assist organizations in maneuvering through highly complex IT and OT environments. Such foresight has only contributed to their strengths, in turn, positioning them as ideal partners to support customers on their risk and digital transformation journeys.
- **Spike in demand for cybersecurity skill sets.** This trend has been observed across most of the MSSPs that participated in the study. Although attrition has significantly impacted the market, there is also a need for specialized domain skill sets in areas such as threat intelligence, security operations management, cloud security, security architecture and assessment, security automation, and OT security. MSSPs are forming strategic alliances with universities and academia among others to train students at an early stage and hire them subsequently. They are also creating ways to engage more with their in-house talent and provide necessary platforms for their personal growth and development through reskilling, upskilling, and cross-skilling activities. This has helped them control the churn rate to a certain extent.
- **Leveraging automation for operational and cost advantage.** Most of the MSSPs in this study started building automation and orchestration capabilities across various aspects of security operations management to standardize security functions, reduce mean time to detect (MTTD) and mean time to respond (MTTR), optimize operational functions, and derive cost and productivity benefits. Vendors are differentiating by automating 25–75% of their security operations, thereby eliminating repetitive tasks, reducing human error, and redirecting skilled resources to high-priority alerts.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

The managed security services market is quite matured, with various providers offering different aspects of the managed security services portfolio along with adjacent services. This study evaluates and analyzes primary players offering managed security services capabilities in Asia/Pacific. IDC narrowed down the field of players based on the following criteria:

- **Managed security services portfolio**. Each SP is required to possess a fairly comprehensive managed security services portfolio, with at least 50% or more matching IDC's scope of managed security services taxonomy, including managed threat intelligence services, MDR services, managed network security services, managed endpoint security services, managed identity and digital trust services, managed secure web gateway services, analytics, intelligence, response, and orchestration services (AIRO), cloud posture and compliance monitoring, and OT/IoT monitoring.
- **Geographic presence**. Each vendor is required to have in-country managed security services delivery capabilities (or presence of a security operations center [SOC]) in a minimum of two Asia/Pacific subregions: North Asia (Japan, Korea), Greater China (China, Hong Kong, and Taiwan), Southeast Asia (Singapore, Malaysia, Thailand, Indonesia, Vietnam, and the Philippines), South Asia (India, Pakistan, Sri Lanka, Bangladesh), and Australia and New Zealand (ANZ).
- **Multipoint assessment completion**. Each participating company is required to complete a multipoint assessment covering a total of 26 capabilities and strategy criteria defined by IDC to be the most conducive to success in delivering managed security services in the Asia/Pacific region.

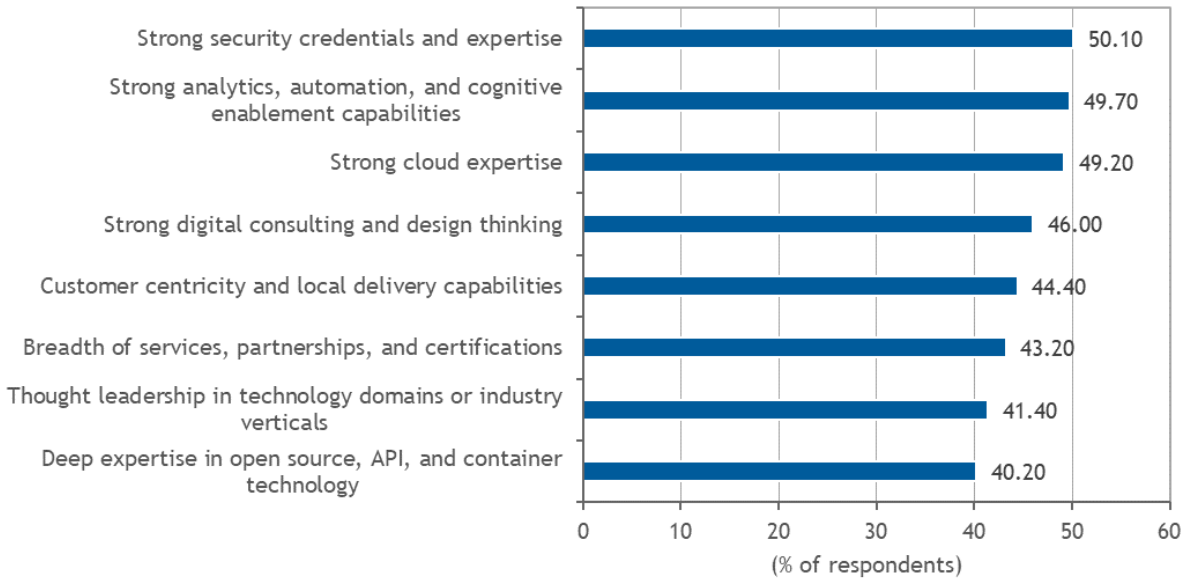
ADVICE FOR TECHNOLOGY BUYERS

Organizations in the region are becoming very specific regarding their expectations from the SPs in the light of increasing IT complexities, expanded threat landscape and regulatory environment and the digital enterprise that is shaping the future. According to IDC's *2022 Asia/Pacific Enterprise Services and Security Sourcing Survey*, the top skills/capabilities that enterprises look for include strong security credentials and expertise, strong analytics, automation, and cognitive enablement capabilities.

FIGURE 2

Top Capabilities When Looking for Next Generation IT SP

Q. Rate how important the following attributes/skills/capabilities are when looking for next generation IT SPs.



Source: IDC Asia/Pacific Enterprise Services and Security Sourcing Survey, July 2022

Although SPs continue to put a lot of emphasis on strengthening technical capabilities, partnerships, and innovation road map, customer centricity is at the crux of all initiatives. The message is clear. The customization of global capabilities to suit local requirements, continuous information and insights sharing, and co-innovating solutions has been the key distinguishing factor that differentiates the visionaries from others.

According to IDC's *2022 Asia/Pacific Enterprise Services and Security Sourcing Survey,* when investing in new and emerging digital technologies, 22% preferred to partner with SPs with deep technical expertise (e.g., research and development [R&D], open source contribution, standards contribution), followed by 21% preferring partners with compliant, secure, and governance expertise and 20.5% opting for partners with deep functional/line-of-business expertise. This demonstrates enterprises' focus on the right skills and capabilities before choosing an SP.

As buyers evaluate MSSPs on different parameters, they should bear in mind the core capabilities identified by IDC. IDC encourages buyers to explore the managed security services capabilities described in the Market Definition section and recommends:

- **Detailed understanding of vendor services portfolio and alignment with enterprise requirement.** Most of the MSSPs that participated in this study offer a fairly comprehensive suite of managed security services. What differentiates them is their ability to customize services based on the industry vertical or digital maturity of the company. Digitally mature companies often require advanced capabilities that require specialized skill sets and investments in innovative technology, whereas organizations that have recently started their digital journey

require much more proactive support, advisory services, and greater involvement from their SPs. Buyers should evaluate their MSSPs based on security maturity. Although most of the MSSPs that participated in the study showcased strong credentials and service offerings, buyers need to also note their capabilities to deliver advanced services, such as risk advisory, threat intelligence, MDR and zero-trust frameworks, SASE, digital forensics, and digital consulting. Conducting pilots or proof of concepts (POC) with MSSPs can also be very helpful in determining what works best for the buyer.

- **Pay close attention to delivery and service capabilities**. Although most vendors have end-to-end capabilities, when it comes to services delivery, regular monitoring, and management, global expertise is often not replicable across regional or local clients because of resource capabilities, customization demands, adherence to regulations, and many other aspects. This creates a great deal of friction once the customer journey starts. Hence, it is advisable to focus on the vendor's regional capabilities, R&D centers, innovation for local markets, and industry use cases. This will help buyers understand and align their strategies with their service partners' road map. Most MSSPs go the partnership/acquisition route to plug the gaps from an industry or geo perspective to build or acquire capabilities. For example, some regulated industries have very niche requirements pertaining to data residency, data privacy, and data sovereignty. In such cases, MSSPs that have tie-ups with local partners will be important to technology buyers.
- **Look for advisory/consultative engagement instead of tactical**. This might not come as a surprise, but with threat environment expanding and perimeters dissolving, it is no longer easy for buyers to defend the attack surface alone. Reimagining the security landscape is a given, and buyers should engage with MSSPs that are willing to work as advisors rather than as transactional partners. Security discussions are becoming more strategic in nature. Hence, it is imperative for technology buyers to share their vision and strategy with their service partners to carve a road map that is aligned accordingly. This might include risk assessment, security architecture reassessment, threat landscape, and regulatory demands, among other facets. Taking a consultative approach will go a long way in bolstering the partnership with relevant process and technology transformation.
- **Integration of automation and threat intelligence capabilities**. Evaluate the SP on its advanced automation and threat management competencies. SPs that have significantly automated security operations and processes will be able to pass on value-added benefits to their clients. Leveraging artificial intelligence/machine learning (AI/ML) and automation, SPs can greatly enhance SOC efficiency and productivity, resulting in faster remediation. Further, MSSPs deepening their threat intelligence capabilities and integrating them with MSS, MDR, and security operation services are better positioned to deliver and maintain service standards. Threat intelligence also feeds into creating and updating playbooks, which helps quicken the threat life-cycle management process.
- **Seamless platforms to provide single pane of glass view**. A key challenge that enterprises face today is the inconsistent view across their IT estate spanning endpoint, network, edge, and cloud environment. SPs that can seamlessly integrate all environments across a single platform for a uniform view will have an edge over other MSSPs. As cybermiscreants think of multiple ways to infiltrate enterprise systems, technology buyers need to look for solutions and services that offer complete visibility and control over their threat environment.
- **Talent and support**. Over the last few quarters, skill set availability and retention have been a major challenge for IT providers. Retaining and upskilling resources across areas such as DevSecOps, governance, risk, and compliance (GRC), cloud security, data engineering, threat analytics, and OT security, will be a key differentiator, and buyers must consider their SPs' talent management strategy to ensure the consistent and seamless delivery of services

without major disruption. Local talent development and management through academic alliances and industry partnerships will also go a long way in establishing the MSSP as a trusted partner.

Organizations should consider SPs that can provide holistic services, ranging from professional and business consulting to MSS, and walk with them on their digital journey as a trusted advisor and partner.

FEATURED VENDOR PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and opportunities.

Tata Communications

According to IDC analysis and buyer perception, Tata Communications is positioned under the Major Players category in the 2022 IDC MarketScape for Asia/Pacific Managed Security Services.

Headquartered in Mumbai, India, Tata Communications is a telecommunications provider that enables a cohesive digital ecosystem powered by cloud, mobility, IoT, collaboration, cybersecurity, and network services. Its cybersecurity services portfolio spans advanced network security, threat management SOC, cloud security, and governance, risk, and compliance management. As a connectivity provider, Tata Communications has witnessed strong uptake for its DDoS protection services, secure web gateway, and threat management.

The vendor has built a strong MDR on an XDR architecture aligned to the MITRE ATT&CK framework, helping it detect and test customer IT environments with various attack techniques and identify anomalies. Apart from integrated threat intelligence and automated orchestration, the vendor leverages its extensive network coverage to supplement endpoint and log data with network threat detection for real-time traffic profiling, north–south and east–west traffic analyses, and application identification.

Managing security across various hybrid and multicloud environments has been a major investment area for enterprises today. Tata Communications differentiates itself by offering a cohesive security architecture across the hybrid digital estate with centralized governance using management tools, processes, and frameworks. It has deep partnerships with AWS, Azure, and Google Cloud Platform (GCP) as well as major third-party security solution providers to enhance coverage and control and build greater credibility with the customers.

To help the MTTD and MTTR and improve proactive detection, the vendor has developed a SOAR platform with over 30 playbooks and 400 use cases engineered on its cloud SIEM platform. This helps its customers access an increasing set of SOAR playbooks aligned with the MITRE framework and derive significant benefits from RPA and SOAR initiatives. The platform also helps automate L1 and L2 activities, thereby saving analyst time significantly.

From a partnership point of view, the vendor evaluates partner's capabilities, local presence, and support, use case deployments, and process maturity to support MSSP partners before forging tie-ups. Further, it has strong alliances in the Confederation of Indian Industry (CII) to drive security awareness in India. It is also an empaneled MSSP in the Indian Computer Emergency Response Team (CERT-

IN) to promote effective security practices and an empaneled CSP for the Ministry of Electronics and Information Technology (MeitY) to deliver cloud services to government and public sector units in India.

A unique differentiating factor for the vendor is its Tata Communications Exchange (TCx) platform, in which the vendor unifies customer experiences and provides a single view to its customers across its digital estate covering network, unified communication and collaboration, cloud, and cybersecurity services. Customers can access the portal from any device using a single sign-on (SSO). Access can be strictly controlled based on roles or set rules. The portal enables customers to track service quality and get a unified view of the security posture through intuitive and feature-rich dashboards.

Strengths

Tata Communications leverages the MITRE framework to build its capabilities and unify siloed technology solutions and services across digital estates, thereby strengthening its cybersecurity posture. The vendor has visibility into large volume of network traffic through its ISP business and network traffic analysis (NTA) feeds into threat intelligence to offer proactive protection to its customers. With an increasing number of cloud deployments, the vendor has been successfully providing better visibility and security across hybrid IT environments with greater regulatory compliance.

According to client feedback, the vendor is extremely proactive in providing regular updates, quick responses, and full support to protect customers from cyberthreats. Its vast network coverage helps detect threats early and provide strong incident management and mitigation services. Its thought leadership in the cybersecurity space and strong MDR and cloud security operations have been well appreciated in the market.

The vendor has a dominant presence in the small and midmarket space. However, with tighter integration across its various portfolio and a stronger platform-centric approach, it is making quick inroads into the enterprise segment, which is fast moving into connected cloud environments for productivity and efficiency benefits.

Tata Communications offers multiple commercial models with flexible options for contracts, billing, and payment frequency. This has been a success, especially across medium-sized enterprises that prefer flexible options along with attractive pricing and business continuity support.

Challenges

Although the vendor has made noteworthy progress to become a trusted one-shop digital ecosystem enabler, there are still areas in capabilities and delivery that require improvement. According to customer feedback, the vendor needs to increase local support teams and capabilities around security analytics and automation. Tata Communications is working toward improving its automation capabilities by adding playbooks for SOAR and use cases for SIEM to improve protection from advanced threats. It is also working on strengthening the skill base to provide augmented XDR services and other add-on services, such as threat hunting, incident response, and forensics.

Customers also expect better collaboration and information sharing from the vendor with respect to threat intelligence and insights and improvement in overall process alignment.

Consider Tata Communications When

With its strong connectivity heritage, Tata Communications is well suited for midsize to large organizations looking for a partner with capabilities across cloud, network, and security services and the ability to deliver a secure connected digital experience.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here, and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis or strategies axis indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represent the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

For the purpose of this study, IDC defines MSS as the round-the-clock management and monitoring of security solutions and activities delivered from an SOC. We include all MSS, whether these involve the management of security solutions deployed on a customer's premises or solutions hosted in a datacenter or cloud external to a customer's premises.

There is a steady stream of new services offered by managed security services providers that extend beyond traditional managed security services solutions, such as managed threat intelligence and MDR, which directly link to an outcome.

LEARN MORE

Related Research

- IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment (IDC #US48761022, September 2022)
- Market Analysis Perspective: Worldwide Security Services, 2022 – 2022 and Beyond (IDC #US47315321, September 2022)
- Southeast Asia IT Services Market Forecast, 2022-2026 (IDC #AP49166922, July 2022)
- IDC Survey Spotlight: How Are Organizations Ramping Up Their Cyber Readiness and Defense Strategies? (IDC #AP49172722, June 2022)
- Securing the Edge: SASE Trends in Asia/Pacific (IDC #AP48491722, June 2022)
- IDC Worldwide CEO Survey 2022: The CEO Tech Agenda in a Digital-First World – An APJ Perspective, Part 1: Big Themes, Business Priorities, and Risks (IDC #AP48503322, May 2022)
- Market Analysis Perspective: Asia/Pacific Security Services (IDC #AP48837622, May 2022)
- IDC's Worldwide Security Services Taxonomy, 2022 (IDC #US48548722, April 2022)

Synopsis

The IDC MarketScape: Asia/Pacific Managed Security Services 2022 Vendor Assessment study evaluates 18 vendors that provide managed security services within the region. The participating firms were meticulously evaluated using the IDC MarketScape model, which reviews the vendors' capabilities and strategies against an extensive list of scoring criteria and parameters. The 26 different market determining criteria included breadth of service offerings, managed detection and response (MDR) and zero-trust capabilities, portfolio benefit, cloud security, services delivery model, marketing/thought leadership, innovation/intellectual property (IP), cost management, customer satisfaction, business performance and employee management, to name a few. With the combination of primary research and IDC's own in-depth industry knowledge and insights, IDC conducted a series of interviews and multipoint assessments with vendors and their clients to comprehensively capture the differentiating factors, strengths, and challenges of each vendor. Following a comprehensive and exhaustive analysis, the results were deliberated with IDC's internal panel of expert analysts, resulting in the positioning in IDC's MarketScape figure. The vendors' position on IDC's MarketScape figure will act as a useful and relevant barometer for Asia/Pacific enterprises that are currently evaluating a trusted security services partner to help them navigate their digital-first journeys.

"Building and maintaining digital trust is crucial for enterprises today as they seek partners that can provide a full breadth of security services with clear transparency and visibility to threats coupled with actionable insights. As the threat landscape expands and evolves, organizations are evaluating managed security SPs with deep technical and industry expertise, extensive threat management, and cyber-risk advisory capabilities, which include managed extended detection and response (MxDR), zero trust, and risk assessment, to align their security strategies with digital-first goals," says Shweta Baidya, senior research manager, IDC Asia/Pacific Services and Security. She adds, "SPs that adopt a consultative approach and can deliver global capabilities customized to local requirements, including regulatory and data sovereignty demands, will certainly have an advantage over the rest. SPs in the region have done a commendable job with understanding the challenges of customers with varied maturity levels across countries and are working in close collaboration with their customers to help them transition into the digital environment."

"With an increasingly challenging threat landscape, coupled with the growing demands of the market, being a successful managed security SP (MSSP) can be a struggle in this digital-first era. Organizations are rapidly looking at the support of an MSSP as an alternative to investing heavily in recruitment and staffing costs to curb the scarcity of cyber professionals. In fact, organizations are sourcing for SPs that will act as an extension of their internal IT and security teams, which can offer further cybersecurity expertise to maintain its security posture. A good MSSP employs and maintains the right toolsets and staff, relays accurate data, and understands its customers' reporting processes. A great MSSP goes beyond all that and partners with its customers to measure success, deliver value-added information, and proactively cater to their business needs," says Christian Fam, research manager, IDC Asia/Pacific Services and Security.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Asia/Pacific Headquarters (Singapore)

83 Clemenceau Avenue
#17-01 UE Square, West Wing
Singapore 239920
65.6226.0330
Twitter: @IDC
blogs.idc.com
www.idc.com